CLAIMS:

1. An electronic voting system, the system comprising:

a voting device configured to generate, in response to a voter selection for each of a plurality of voters an encrypted electronic ballot and a printed ballot, both having voter selection data indicating a said voter's choice, said electronic ballot including information to link it to said printed ballot and said printed ballot including information to link it to said electronic ballot;

an electronic vote decryption system configured to receive electronic ballots from said voting device and to decrypt said encrypted electronic ballots including said linking information; and

a voting verification system configured to receive decrypted voter selection data and linking information from said vote decryption system, to receive voter selection data and linking information from said printed ballots and to compare voters choices for a sample of said printed and electronic ballots linked by said linking information, to verify the voting.

2. An electronic voting system as claimed in claim 1 further comprising a ballot box to receive said printed ballots, and a printer coupled to said voting device to print a said printed ballot for verification by a voter prior to reception of said printed ballot by said ballot box.

3. An electronic voting system as claimed in claim 2 wherein said ballot box includes means to select a sample of said printed ballots for said voting verification system.

4. An electronic voting system as claimed in claim 1, 2 or 3 wherein said linking information included with said printed ballot is printed onto said ballot such that it is not directly readable by a human.

5. An electronic voting system as claimed in any one of claims 1 to 4 wherein said sample comprises a predetermined number of ballots, preferably at least 190, more preferably at least 450.

6. An electronic voting system as claimed in any preceding claim wherein said voter verification system is further configured to determine that all said printed ballots carry different linking information, that each said printed ballot links to an electronic ballot, and that the number of printed ballots is the same as the number of electronic ballots.

7. An electronic voting system as claimed in any one of claims 1 to 6 wherein a said encrypted electronic ballot includes voting district identification information, and wherein said comparing of printed and electronic ballots is performed for a selected said district.

8. An electronic voting system as claimed in any preceding claim wherein a said electronic ballot includes voter identification information, and wherein said vote decryption is further configured to separate said voter selection data from said voter identification information prior to providing said voter selection data to said voting verification system.

9. An electronic voting system as claimed in claim 8 wherein said separating comprises a mix-net shuffle operation to provide at least one shuffle of said voter selection data.

10. An electronic voting system as claimed in claim 9 wherein said shuffle operation provides a plurality of shuffles in which each shuffle has a share of a secret key, and in which each shuffle partially decrypts said encrypted electronic ballots using said secret key share.

11. An electronic voting system as claimed in claim 9 or 10 wherein said decryption system includes at least one first server to implement said mix-net, and at least one

second server to provide verification data to demonstrate that a said shuffle does not modify a said voter's choice.

12. An electronic voting system as claimed in claim 11 wherein said verification data comprises a zero-knowledge proof, and further comprising an audit system to output audit data, said audit system including a homomorphic verification system to operate on said verification data from said plurality of shuffles to count votes with verified zero-knowledge proofs without decrypting a said encrypted electronic ballot.

13. An electronic voting system as claimed in any preceding claim further comprising means to process write-in-votes.

14. An electronic voting system as claimed in any preceding claim further comprising a signer to sign a said electronic ballot, said signer being coupled to said voting device and configured only to produce a digital signature for a said electronic ballot in response to input of at least two items of voter authentication.

15. A computer system for verifying an electronic voting system as claimed in claim 1, the computer system comprising:

data memory operable to store data to be processed;

program memory storing processor implementable instructions; and

a processor coupled to said data memory and to said program memory to load and implement said instructions, the instructions comprising instructions for controlling the processor to:

receive decrypted voter selection data and linking information from said vote decryption system;

receive voter selection data and linking information from said printed ballots; and

compare voters choices for a sample of said printed and electronic ballots linked by said linking information to verify the voting.

16. A computer system as claimed in claim 15 wherein said instructions further comprise instructions for controlling the processor to:

determine that all said printed ballots carry different linking information;

determine that each said printed ballot links to an electronic ballot; and

determine that the number of printed ballots is the same as the number of electronic ballots;

to thereby verify said voting.

17. A carrier carrying the processor implementable instructions of claim 15 or 16.

18. A device for collecting ballots, in particular for the electronic voting system of claim 1, the device comprising:

a ballot input to accept a ballot submitted by a user;

a first ballot holder for holding ballots for checking;

a second ballot holder; and

a user interface to allow said user to signal to the device an intention to submit said ballot; and

a selector responsive to said signal to select substantially at random one of said first and second ballot holders to receive said submitted ballot.

19. A claim as claimed in claim 18 further comprising a ballot reader to read information on a said ballot linking the ballot to an electronic ballot; and wherein in response to said signal the device is configured to select a said ballot holder, to indicate said selection to said user, and then to read said linking information on ballot.

20. A printed ballot for an electronic voting system configured to count electronic ballots corresponding to printed ballots, said printed ballot bearing information linking the ballot to a said electronic ballot and information to allow a voter to identify one or more choices, the printed ballot being configured or configurable such that said linking information and said choice identification information are both visible, but not simultaneously.

21. A printed ballot as claimed in claim 20 wherein said linking information and said choice identification information are on opposite sides of said ballot.

22. A method of operating an electronic voting system, the method comprising:

collecting a vote from a voter;

outputting vote as both an encrypted electronic ballot and a printed ballot, each of said printed and encrypted electronic ballots bearing information linking it to the other;

displaying the printed ballot to the voter;

collecting the printed ballot;

repeating said collecting, outputting, displaying and collecting for a plurality of other voters;

decrypting and counting said electronic ballots;

selecting a sample of said printed or electronic ballots and reading voter choices for said sample;

reading voter choices for electronic or printed ballots linked to said selected ballots by said linking information; and

comparing said voter choices read from said sample and said linked ballots to verify a result of said voting.

23. A method as claimed in claim 22 wherein said encrypted distance ballots are homomorphically encrypted, the method further comprising repeatedly permuting and re-encrypting said electronic ballots prior to said decrypting; and verifying said result using a homomorphic verification system.

24. A method as claimed in claim 23 wherein said verifying comprises verifying the correctness of said linking information.

25. A method as claimed in claim 23 or 24 wherein said repeated permuting and re-encrypting further comprises partial decryption of a said electronic ballot.

26. A method as claimed in any one of claims 23 to 25 further comprising producing and verifying a zero-knowledge proof of said repeated permuting, re-encrypting and, when dependent on claim 25, said partial decryption.

27. Computer program code, in particular on a carrier, to implement the method of any one of claims 22 to 26.

28. A method of committing to an electronic data value, the method comprising selecting a substantially random number and a sub group of the multiplication group Z^*_n of integers computed modulo n where n is a product of two primes for the electronic data value and/or said substantially random number and determining a commitment value from said electronic data value and said substantially random number using said subgroup.

29. A method of providing information for verifying correctness of a permutation of encrypted messages performed using one or more data processing entities, the method comprising:

sending a commitment (c_s) to a first set of values (π) defining said permutation to a verifier;

receiving a second set of values (t) from said verifier;

permuting said second set of values with said permutation;

sending a commitment (c_t) to said permuted second set of values to said verifier; and

sending additional information to said verifier for verifying correctness of said permutation, said additional information verifying that said second set of values was permuted with said permutation.

30. A method as claimed in claim 29 wherein said sending of additional information comprises:

receiving a pair of challenge values (λ, x) from said verifier;

determining a third set of values (a) from said permutation, said second set of values and said pair of challenge values and sending a commitment (c_a) to said third set of values to said verifier;

determining and sending a commitment (c_d) to a fourth set of random values (d) to said verifier;

determining a fifth set of random values (Δ) and sending a commitment (c_Δ) to a combination of said fourth and fifth sets of values to said verifier;

sending a check value (E) derived from a further random value (R) to said verifier;

receiving a further challenge value (e) from said verifier; and

sending values (f, z, Z) determined from said further challenge value, said pair of challenge values, said further random value, and said permutation to said verifier;

whereby said verifier is able to verify said correctness using a zero-knowledge protocol.

31. A method of providing information for verifying correctness of a combined permutation and partial decryption of encrypted messages performed using one or more data processing entities, the method comprising:

sending information to said verifier for verifying correctness of said combined permutation and partial decryption, said information comprising information to enable said verifier to verify said performance using a zero-knowledge protocol.

32. A method as claimed in claim 31 wherein said information sending comprises:

sending a commitment (c_s) to a first set of values (π) defining said permutation to a verifier;

receiving a second set of values (t) from said verifier;

permuting said second set of values with said permutation;

sending a commitment (c_t) to said permuted second set of values to said verifier;

receiving a pair of challenge values (λ, x) from said verifier;

determining a third set of values (a) from said permutation, said second set of values and said pair of challenge values and sending a commitment (c_a) to said third set of values to said verifier;

determining and sending a commitment (c_d) to a fourth set of random values (d) to said verifier;

sending a triplet of check values (D, U, V) derived from a pair of random values (d, R) to said verifier;

receiving a further challenge value (e) from said verifier; and

sending values (f, z, Z) determined from said further challenge value, said pair of challenge values, one of said pair of random values, and said permutation to said verifier.

33. A method of shuffling and decrypting encrypted electronic data using a plurality of data processing entities, each entity having a share of a secret key, the method comprising, at each of said entities, partially decrypting and re-randomising said electronic data using said secret key share such that a final said data processing utility fully decrypts said data.

34 A method as claimed in claim 33 further comprising shuffling said electronic data and generating a shuffle proof for verifying said shuffling at each said data processing entity.

35. A method as claimed in claim 34 further comprising verifying each said shuffle with one or more data processing entities.

36. A method, in a computer system, of providing data for verifying that messages of a set of messages provided from a corresponding set of entities are authentic, the method comprising:

selecting, for each said entity, first second and third random numbers;

determining, for each said entity, first and second verification values from, respectively, said first and second random numbers and said entity's message, and said first and third random numbers; and

outputting, for each entity, said entity's message and said first and second verification values.

37. A method for providing data for verification systems for verifying that messages $m_1,..,m_k$ are authentic using a homomorphic verification system without revealing their origin, the method comprising entities $\{E_j\}$ producing the messages each choosing random numbers e_j, r_j and ρ_j and submitting m_j, $V(e_j, r_j)$ anonymously to one entity (entity A) and $V(m_j e_j, \rho_j)$ to another entity (entity B) where V is a verification function, in particular a homomorphic function, in such a way that the messages are authenticated.

38. A method for verifying messages using data provided as claimed in claim 37 wherein the authenticity of $\{m_j\}$ is verified by having entity B submitting $\Pi V(e_j, r_j)^{m_j}$ to entity A, which computes $C = \Pi V(m_j e_j, \rho_j)^{-1} V(e_j, r_j)^{m_j}$, then an entity which knows a secret key for V verifying that C is a commitment to zero.

39. Use of the method of claim 37 or 38 to check write-in votes outputted from a MIX net.

40. Use of the method of claim 37 or 38 for proving correctness of electronic votes in a voting system.

41. Use of the method of claim 37 or 38 for verifying correctness of encrypted information linking electronic ballots to paper ballots.

42. Computer program code to, when running, implement the method of any one of claims 28 to 38.

43. A carrier carrying the code of claim 42.